Certain Subgroups of the Betti-Mathieu Group.

By L. E. Dickson.

1. It was shown in the writer's Dissertation* that the transformation in one variable.

$$X' = \sum_{i=1}^{m} A_i X^{p^{n(m-i)}} \tag{A}$$

represents a substitution upon the marks of the Galois Field of order p^{nm} if, and only if, the determinant

$$|A| \equiv \begin{vmatrix} A_1 & A_2 & \ldots\ldots & A_m \\ A_2^{p^n} & A_3^{p^n} & \ldots\ldots & A_1^{p^n} \\ A_3^{p^{2n}} & A_4^{p^{2n}} & \ldots\ldots & A_2^{p^{2n}} \\ \ldots & \ldots & \ldots & \ldots \\ A_m^{p^{n(m-1)}} & A_1^{p^{n(m-1)}} & \ldots\ldots & A_{m-1}^{p^{n(n-1)}} \end{vmatrix}$$

does not vanish in the Field. The totality of substitutions (A) form a group studied by Betti (for $n=1$) and by Mathieu. This Betti-Mathieu Group was proven in the dissertation cited to be identical with Jordan's group of all linear homogeneous substitutions on m indices,

$$\xi_i' = \sum_{j=1}^{m} \alpha_{ij} \xi_j \qquad (i = 1, \ldots\ldots, m)$$

belonging the $GF[p^n]$. In setting up certain subgroups of the Betti-Mathieu Group, we make use of the following formula, holding for any integer k and quantity X such that $X^{p^{nm}} \equiv X$:

$$\left\{ \sum_{i=1}^{m} A_i X^{p^{n(m-i)}} \right\}^{p^{nk}} \equiv \sum_{i=1}^{m} A_{i+k}^{p^{nk}} X^{p^{n(m-i)}}, \qquad (\text{mod } p), \tag{1}$$

where the subscripts to A_{i+k} are taken modulo m.

* Annals of Mathematics, pp. 65–120, and pp. 161–183, 1897.

2. Consider the subgroup of the Betti-Mathieu Group defined by the relative invariant, in which B belongs to the $GF\,[p^{nm}]$,

$$Z \equiv \sum_{j=0}^{m-1} (BX)^{p^{nj}}.$$

Applying to Z the substitution (A), we have, by (1),

$$Z' \equiv \sum_{j=0}^{m-1} (BX')^{p^{nj}} = \sum_{j=0}^{m-1} \left\{ B^{p^{nj}} \sum_{i=1}^{m} A_{i+j}^{p^{nj}} X^{p^{n(m-i)}} \right\}.$$

The conditions for the identity $Z' = \rho Z$ are, therefore,

$$\sum_{j=0}^{m-1} B^{p^{nj}} A_{i+j}^{p^{nj}} = \rho B^{p^{n(m-i)}}, \qquad (i = 1, 2, \ldots, m). \qquad (2)$$

Raising (2) to the power p^n and setting $l = j + 1$, we find

$$\sum_{l=1}^{m} B^{p^{nl}} A_{i+l-1}^{p^{nl}} \equiv \sum_{l=1}^{m-1} B^{p^{nl}} A_{i+l-1}^{p^{nl}} + BA_{i-1} = \rho^{p^n} B^{p^{n(m-i+1)}}$$

Changing the summation index from l to j, we have

$$\sum_{j=0}^{m-1} B^{p^{nj}} A_{i+j-1}^{p^{nj}} = \rho^{p^n} B^{p^{n(m-i+1)}} \qquad (3)$$

Aside from the factor ρ^{p^n}, formula (3) is identical with the $(i-1)^{\text{st}}$ formula of the set (2). A condition for the invariance of the function Z is that the factor ρ satisfy the equation

$$\rho^{p^n} = \rho.$$

With this restriction upon ρ, all of the m formulæ (2) are consequences of a single one of them, say that given by $i = m$. We may thus enunciate the following

Theorem: *The totality of substitutions* (A) *for which*

$$\rho \equiv B^{-1} \sum_{j=0}^{m-1} B^{p^{nj}} A_j^{p^{nj}}$$

is a mark of the $GF\,[p^n]$ *form a group whose substitutions multiply the function* Z *by the parameter* ρ.

Note.—Since the function Z belongs to the $GF[p^n]$, the corresponding linear group is that subgroup of the general m-ary linear homogeneous group in the $GF[p^n]$ which leaves relatively invariant a certain linear function Z of the m variables.

3. By way of illustration of the general developments of §4, we consider the special case of the group of substitutions in the $GF[p^{3n}]$ on the variable X,

$$X' = A_1 X^{p^{2n}} + A_2 X^{p^n} + A_3 X,$$

which multiply by a parameter ρ the function

$$Y \equiv X X^{p^n} + X^{p^n} X^{p^{2n}} + X^{p^{2n}} X.$$

To form the transformed function Y', we note that

$$X' X'^{p^n} = A_3 A_1^{p^n} X^2 + (A_3^{p^n+1} + A_2 A_1^{p^n}) X^{p^n+1} + A_2 A_3^{p^n} X^{2p^n}$$
$$+ (A_3 A_2^{p^n} + A_1^{p^n+1}) X^{p^{2n}+1} + (A_2^{p^n+1} + A_1 A_3^{p^n}) X^{p^{2n}+p^n} + A_1 A_2^{p^n} X^{2p^{2n}}.$$

Raising this equation to the powers p^n and p^{2n} and adding the three results, we find that the conditions for the identity

$$Y' \equiv X' X'^{p^n} + X'^{p^n} X'^{p^{2n}} + X'^{p^{2n}} X' = \rho Y$$

are the following six relations:

$$f \equiv A_3^{p^n+1} + A_2 A_1^{p^n} + A_3^{p^n} A_2^{p^{2n}} + A_1^{p^{2n}+p^n} + A_2^{p^{2n}+1} + A_1^{p^{2n}} A_3 = \rho, \tag{4}$$

$$f^{p^n} = \rho, \qquad f^{p^{2n}} = \rho, \tag{5}$$

$$A_3 A_1^{p^n} + A_1^{p^n} A_2^{p^{2n}} + A_2^{p^{2n}} A_3 = 0, \tag{6}$$

together with (6) raised to the powers of p^n and p^{2n}.

Those substitutions in which the marks A_1, A_2, A_3 of the $GF[p^{3n}]$ satisfy the condition (6) *and give to the function f a value belonging to the $GF[p^n]$, form a group leaving Y invariant up to the factor f.*

4. Consider the substitutions (A) of the Betti-Mathieu Group which leave relatively invariant the function

$$Y_s \equiv \sum_{j=0}^{m-1} (BX)^{p^{nj}} (CX)^{p^{n(s+j)}},$$

where B, C and X belong to the $GF[p^{nm}]$ and s is any integer $< m$. We observe that

$$Y_s^{p^n} = Y_s,$$

so that Y_s belongs to the $GF[p^n]$. Applying to Y_s the substitution (A) and making use of formula (1), we find that

$$\left.\begin{aligned} Y'_s &\equiv \sum_{j=0}^{m-1} (BX')^{p^{nj}} (CX')^{p^{n(s+j)}} \\ &= \sum_{j=0}^{m-1} B^{p^{nj}} C^{p^{n(s+j)}} \sum_{i,\,l}^{1\ldots\ldots m} A_{i+j}^{p^{nj}} A_{l+s+j}^{p^{n(s+j)}} X^{p^{n(m-i)}} X^{p^{n(m-l)}} \end{aligned}\right\}$$
$$= \sum_{i=1}^{m} D_{ii} X^{2p^{n(m-i)}} + \sum_{i<l}^{i,\,l=1\ldots\ldots m} D_{il} X^{p^{n(m-i)}} X^{p^{n(m-l)}},$$

where we have used the abbreviations

$$D_{ii} \equiv \sum_{j=0}^{m-1} B^{p^{nj}} C^{p^{n(s+j)}} A_{i+j}^{p^{nj}} A_{i+s+j}^{p^{n(s+j)}},$$
$$D_{il} \equiv \sum_{j=0}^{m-1} B^{p^{nj}} C^{p^{n(s+j)}} \left(A_{i+j}^{p^{nj}} A_{l+s+j}^{p^{n(s+j)}} + A_{l+j}^{p^{nj}} A_{i+s+j}^{p^{n(s+j)}}\right).$$

The subscripts to D_{il}, like those to A_i, are to be taken modulo m.

4_1. Suppose first that s is neither 0 nor $m/2$. The powers of X in the terms of Y_s have, then, distinct exponents. We may write Y_s in the form

$$Y_s \equiv \sum_{i=1}^{m-s} (BX)^{p^{n(m-i-s)}} (CX)^{p^{n(m-i)}} + \sum_{i=1}^{s} (BX)^{p^{n(m-i)}} (CX)^{p^{n(s-i)}}.$$

The identity $Y'_s = \rho Y_s$, where ρ is a parameter, thus imposes upon the coefficients A_i the following conditions:

$$D_{ii} = 0, \qquad (i = 1,\ 2,\ \ldots\ldots,\ m) \qquad (7)$$
$$D_{i\,i+s} = \rho B^{p^{n(m-i-s)}} C^{p^{n(m-i)}}, \qquad (i = 1,\ \ldots\ldots,\ m-s) \qquad (8)$$
$$D_{i\,i+m-s} = \rho B^{p^{n(m-i)}} C^{p^{n(s-i)}}, \qquad (i = 1,\ \ldots\ldots,\ s) \qquad (9)$$
$$D_{il} = 0. \qquad \begin{pmatrix} i,\ l = 1,\ \ldots\ldots,\ m;\ i < l \\ l \neq i,\ i+s,\ \text{or } i+m-s \end{pmatrix} \qquad (10)$$

We verify immediately that

$$D_{il}^{p^n} = D_{i-1\,l-1}. \qquad (11)$$

The conditions (7) thus reduce to a single one, as $D_{11} = 0$. The conditions (8) are consequences of a single one, in view of (11), provided ρ satisfies the relation $\rho^{p^{n}} = \rho$. Similarly for the conditions (9). Further, we may verify that the ρ calculated from (8) equals $\rho^{p^{ns}}$ as calculated from (9). Hence (8) and (9) reduce

to the single condition that the value for ρ shall belong to the $GF[p^n]$. Finally, the $\frac{1}{2}m(m-1)-m$ conditions (10) reduce to $\frac{1}{2}(m-3)$ or $\frac{1}{2}(m-2)$ according as m is odd or even. Indeed, by (11), we may retain only the conditions $D_{1l}=0$. From the symmetry of D_{il}, it equals D_{li}. Hence from $D_{1l}=0$ follows $D_{l1}=0$, and by (11), $D_{1\,m+2-l}=0$.

The two equivalent equations of one pair,

$$D_{1l}=0,\quad D_{1\,m+2-l}=0,\quad \left(\begin{array}{l} l=2,\ldots\ldots, m,\ l\neq 1+s, \\ \qquad\qquad\qquad l\neq 1+m-s \end{array}\right) \tag{12}$$

are identical only when $l=\frac{1}{2}(m+2)$, i. e., when m is even. The two equations excluded in (12),

$$D_{1\,1+s}=0,\quad D_{1\,1+m-s}=0,$$

would have formed a pair of equivalent equations. There remain $\frac{1}{2}(m-3)$ pairs if m be odd and $\frac{1}{2}(m-4)$ pairs with an additional middle equation if m be even. We have proven the theorem:

For $s\neq 0$, $\neq \frac{m}{2}$, the number of independent conditions upon the m coefficients A_i of a substitution (A) *in order that it leave relatively invariant the function Y_s is at most*

$$\tfrac{1}{2}(m+1)\ \textit{for } m \textit{ odd},$$
$$\tfrac{1}{2}(m+2)\ \textit{for } m \textit{ even}.$$

4_2. For $s=0$, we may give Y_s the form

$$Y_0\equiv\sum_{i=1}^{m}(BC)^{p^{n(m-i)}}X^{2p^{n(m-i)}}$$

The conditions for the invariance of Y_0 are, therefore,

$$D_{ii}=\rho\,(BC)^{p^{n(m-i)}},\qquad (i=1,2,\ldots\ldots,m) \tag{13}$$
$$D_{il}=0.\qquad (i,\ l=1,\ldots\ldots,m;\ i<l) \tag{14}$$

As before, we derive from (13) the condition $\rho^{p^n}=\rho$, in virtue of which the conditions (13) reduce to a single one. The conditions (14) reduce to $\frac{1}{2}(m-1)$ if m be odd, and to $\frac{1}{2}m$ if m be even. The above theorem, therefore, holds true if $s=0$.

4_3. If $s=m/2$, the terms in Y_s have in pairs like powers of X, viz., the j^{th} and $s+j^{\text{th}}$. The conditions become more complicated.

5. To the groups in §§3–4 there correspond certain linear homogeneous m-ary groups defined by single quadratic invariants. Indeed, if I be a root of a congruence of degree m belonging to and irreducible in the $GF[p^n]$, we may set

$$X=\sum_{j=0}^{m-1}\xi_j I^j, \quad B=\sum_{j=0}^{m-1}\beta_j I^j, \quad C=\sum_{j=0}^{m-1}\gamma_j I^j,$$

where ξ_j, β_j and γ_j are marks of the $GF[p^n]$. Then, for example, $(BX)^{p^n}$ becomes a *linear* function of $\xi_0, \xi_1, \ldots, \xi_{m-1}$, since

$$\xi_j^{p^n}=\xi_j.$$

Hence Y_8 becomes a quadratic function of the ξ's. As noted above, Y_8 belongs to the $GF[p^n]$. Hence our quadratic function of the ξ's has for coefficients certain marks of the $GF[p^n]$. The corresponding m-ary linear group is, therefore, defined by a single quadratic invariant. The structure of all such groups has been fully determined by the writer in the American Journal of Mathematics for July, 1899.

THE UNIVERSITY OF TEXAS, *July* 14, 1899.